infra STRUKTUR

2-Faktor Authentifizierung

Erhöhen Sie die Sicherheit Ihrer Login-Daten

Was ist die 2-Faktor-Authentifizierung (2FA)?

Mit dieser Authentifizierungsmethode können Sie die Sicherheit Ihres Logins erhöhen. Zusätzlich zu Benutzername und Passwort wird dann bei der Anmeldung zu Ihrer „infra-struktur“ ein weiterer, wechselnder *Schlüssel* mit abgefragt, bevor Sie Zugang zu Ihrer „infra-struktur“ erhalten.

Für wen ist die 2-Faktor-Authentifizierung sinnvoll?

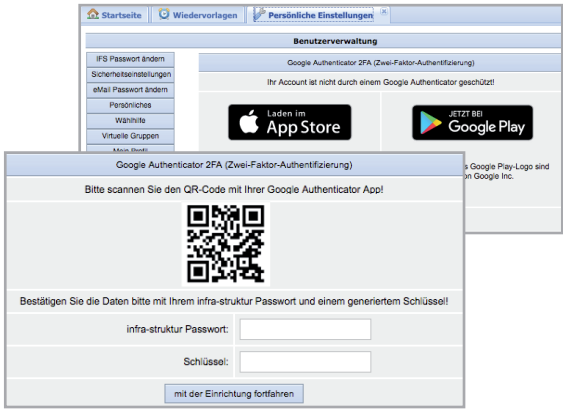
Die 2FA ist sinnvoll, wenn Sie sich häufig an fremden Rechnern einloggen oder wenn Ihr PC auch für andere zugänglich ist. Mit der 2FA minimieren Sie das Risiko, dass Dritte Ihre Login-Daten ungewollt verwenden.

EINRICHTUNG

1

Google App „Authenticator“ auf Ihrem Smarthphone installieren

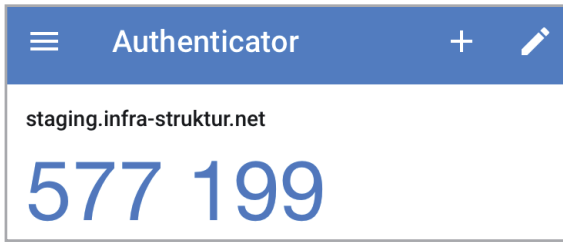
Sie können die 2FA unter Einstellungen -> persönliche Einstellungen -> Sicherheitseinstellungen selbst aktivieren und deaktivieren. Installieren Sie zunächst die kostenfreie App „Google Authenticator“ auf Ihrem Smartphone. Damit nicht Fremde an Ihrem Rechner die 2FA manipulieren können, geben Sie zunächst Ihr infra-struktur Passwort ein. Jetzt erzeugt infra-struktur automatisch einen QR-Code. Scannen Sie diesen mit dem Handy ab, um die Einrichtung der App abzuschließen.



2

6-stelligen Schlüssel erzeugen

Die App auf Ihrem Smartphone erzeugt nun alle 30 Sekunden eine 6-stellige Zahl, die in Zukunft neben dem Benutzernamen und dem Passwort, zusätzlich abgefragt wird. Wichtig: dieser 6-stellige Schlüssel kann nur einmal verwendet werden und wechselt alle 30 Sekunden!



3

2FA anwenden

Ist die 2FA aktiviert, werden Sie zukünftig beim Login gebeten, zusätzlich zu Benutzername und Passwort auch den Schlüssel einzugeben. Öffnen Sie dazu einfach die App auf Ihrem Smartphone und geben den angezeigten Code ein. Damit Sie nicht bei jedem Login den wechselnden Schlüssel eingeben müssen, gibt es die Option „Auf diesem Computer für 7 Tage merken“.